SOPHOS

L'ÉTAT DE LA SÉCURITÉ DU CLOUD 2020

Résultats d'une enquête indépendante menée auprès de 5 000 responsables informatiques hébergeant des données et des ressources dans le Cloud public.

Livre blanc Sophos Juillet 2020

Introduction

Face à la demande croissante de travail à distance et de services de Cloud public, les infrastructures sur site deviennent petit à petit une contrainte pour les entreprises. Migrer vers le Cloud a cependant un coût : l'augmentation de la surface d'attaque des entreprises. Bien que les nombreuses attaques très médiatisées de services de stockage en ligne aient permis de sensibiliser à la sécurité du Cloud, les cybercriminels continuent de déployer des efforts considérables pour garder une longueur d'avance.

Pour comprendre la réalité derrière ces gros titres, Sophos a commandé une enquête indépendante auprès de 3 251 responsables informatiques utilisant le Cloud public, répartis dans 26 pays. Ces résultats apportent un éclairage nouveau sur les préoccupations des équipes de sécurité qui hébergent des données et des ressources dans le Cloud public et sur la manière dont les attaquants innovent pour trouver de nouvelles façons de pénétrer dans les environnements. Cette étude offre également des conseils pour vous aider à trouver la visibilité dont vous avez besoin — et peut-être les failles de sécurité dont vous ignoriez l'existence.

À propos de l'enquête

Sophos a chargé le cabinet d'étude Vanson Bourne de mener une enquête auprès de 3 521 responsables informatiques hébergeant actuellement des données et des ressources dans le Cloud public. Par 'Cloud public', nous entendons au moins l'un des fournisseurs suivants : Azure, Oracle Cloud, AWS, VMWare Cloud on AWS et Alibaba Cloud. Par ailleurs, ils peuvent également utiliser Google Cloud et IBM Cloud. Sophos n'a joué aucun rôle dans la sélection des répondants et toutes les réponses ont été fournies de manière anonyme. Cette enquête s'est déroulée entre janvier et février 2020.

48 % des répondants travaillent pour des entreprises de 100 à 1 000 employés et 52 % pour des entreprises de 1 001 à 5 000 employés.

Les répondants proviennent de 26 pays répartis sur 6 continents :

PAYS	NB DE RÉPONDANTS	PAYS	NB DE RÉPONDANTS	PAYS	NB DE RÉPONDANTS
Australie	148	Inde	227	Singapour	158
Belgique	66	Italie	128	Afrique du Sud	158
Brésil	136	Japon	126	Espagne	139
Canada	131	Malaisie	79	Suède	72
Chine	162	Mexique	140	Turquie	72
Colombie	120	Pays-Bas	150	EAU	65
République tchèque	63	Nigeria	65	Royaume-Uni	191
France	203	Philippines	62	États-Unis	413
Allemagne	194	Pologne	53		

Les répondants couvrent un large éventail de secteurs industriels, tant publics que privés.

SECTEUR	NB DE RÉPONDANTS	% DE RÉPONDANTS
IT, technologies et télécoms	735	21%
Manufacture et production	466	13%
Commerce, distribution et transport	449	13%
Services financiers	409	12%
Services commerciaux et professionnels	357	10%
Secteur public	308	9%
Construction et immobilier	177	5%
Énergie, pétrolier/gazier, services publics	125	4%
Médias, loisirs et divertissement	120	3%
Autre	375	11%

Résumé

Cette étude apporte un nouvel éclairage sur les expériences des entreprises ayant été attaquées par des cybercriminels dans le Cloud public, notamment :

- **Près de 3/4 des entreprises hébergeant des données et des ressources dans le Cloud public ont déploré un incident de sécurité au cours de l'année passée.** 70 % des entreprises ont été victimes d'un malware, d'un ransomware, d'un vol de données, d'une tentative de compromission de compte ou du cryptojacking l'an dernier.
- **La perte/fuite de données est la principale préoccupation des entreprises.** En effet, 44 % des entreprises placent la perte de données parmi leurs trois principales sources de préoccupations.
- **96 % des entreprises sont préoccupées par leur niveau de sécurité Cloud actuel.** La perte de données, la détection et la réponse, et la gestion de plusieurs plateformes Cloud sont les trois principales préoccupations des entreprises.
- **Les entreprises utilisant plusieurs plateformes Cloud ont signalé un plus grand nombre d'incidents de sécurité au cours des 12 derniers mois.** 73 % des entreprises interrogées utilisent 2 plateformes de Cloud public ou plus, et ont déclaré davantage d'incidents de sécurité que celles n'en utilisant qu'une seule.
- **Grâce au Règlement général sur la protection des données (RGPD), les entreprises européennes affichent les taux d'attaques les plus bas de l'enquête.** Les directives du RGPD mettent l'accent sur la protection des données, et la médiatisation de certaines attaques de ransomware a certainement poussé les cibles les plus lucratives en Europe à durcir leur sécurité.
- **Seule 1 entreprise sur 4 considère le manque de compétences du personnel comme une préoccupation majeure, malgré le nombre de cyberattaques signalées dans l'enquête.** Pour durcir les postures de sécurité dans le Cloud, il est crucial d'avoir les compétences nécessaires pour créer des modèles architecturaux adaptés, développer des cas d'usages clairs et exploiter des services tiers pour les outils de la plateforme. Pourtant, ces compétences sont sous-estimées.
- **2/3 des entreprises laissent des portes dérobées (backdoors) ouvertes aux attaquants.** L'exposition accidentelle de données à cause d'erreurs de configuration continue de gangréner les entreprises. Les failles de sécurité ainsi créées ont été exploitées dans 66 % des attaques (soit en exploitant une faille dans le pare-feu d'applications Web pour obtenir des identifiants de compte, soit en exploitant des ressources mal configurées), tandis que 33 % des attaques ont utilisé des identifiants volés pour accéder aux comptes des fournisseurs Cloud.

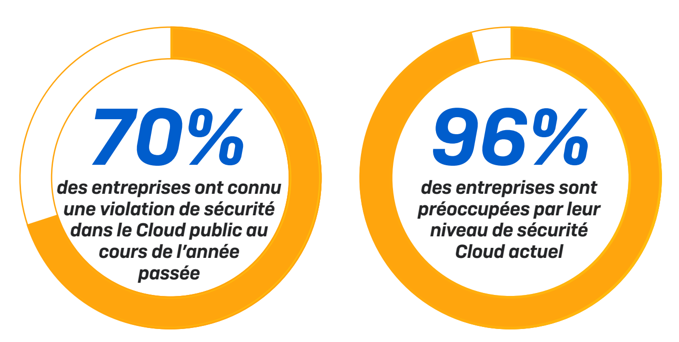
Utilisation des données et des graphiques

Nous encourageons la réutilisation des données, graphiques et textes publiés dans ce rapport. Vous êtes libre de partager ce travail et de l'utiliser à des fins commerciales tant que vous créditez le présent rapport de Sophos « L'état de sécurité du Cloud 2020 ».

Partie 1 : La prévalence des attaques dans le Cloud

7 entreprises sur 10 ont été touchées par une cyberattaque

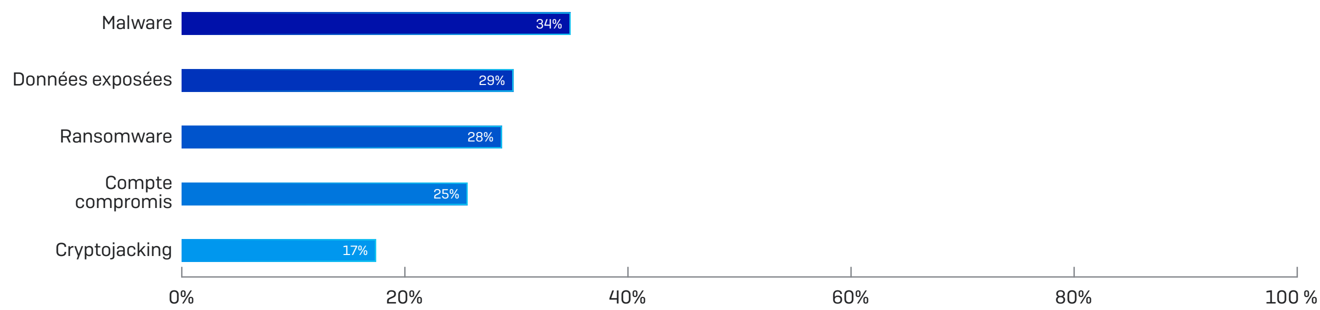
70 % des répondants ont déclaré avoir subi une violation de sécurité dans le Cloud public au cours de l'année passée. Les entreprises sont extrêmement préoccupées par cette situation, puisque 96 % des 3 521 répondants ont exprimé des inquiétudes quant à leur niveau de sécurité actuel sur les 6 principales plateformes de Cloud public, notamment Amazon Web Services, Microsoft Azure et Google Cloud Platform.



Différents environnements, mêmes types d'attaque

En analysant les différents types de cyberattaque ciblant le Cloud, nous nous sommes rendu compte que nous avons affaire aux suspects habituels : 50 % des entreprises ont été touchées par un malware sous une forme ou une autre, y compris des ransomwares (les répondants pouvaient choisir plusieurs options).

Entreprises ayant connu un incident de sécurité au cours de l'année passée

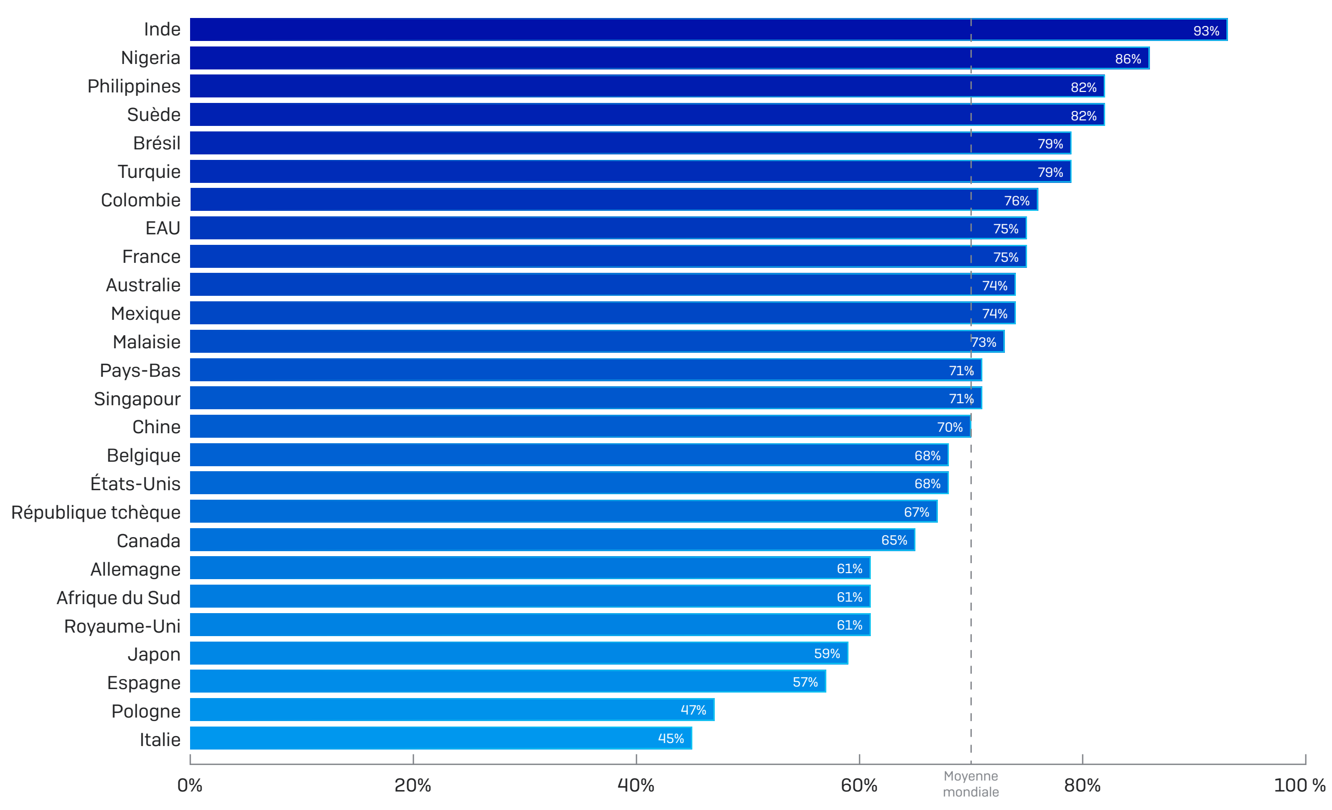


Votre entreprise a-t-elle subi un incident de sécurité dans le Cloud public au cours des 12 derniers mois ? Base de 3 521 répondants.

Le nombre d'attaques varie selon les pays

L'analyse du nombre d'attaques ciblant le Cloud public à travers le monde révèle des variations intéressantes. Cela est probablement dû au fait que les cybercriminels concentrent leurs efforts là où se trouvent les plus grandes opportunités de réussite. Les analyses par pays ont également montré des variations dans les niveaux de protection et de visibilité des environnements Cloud, la connaissance des responsabilités de chacun dans le Cloud et des bonnes pratiques de sécurité.

Entreprises ayant connu un incident de sécurité dans le Cloud public au cours de l'année passée



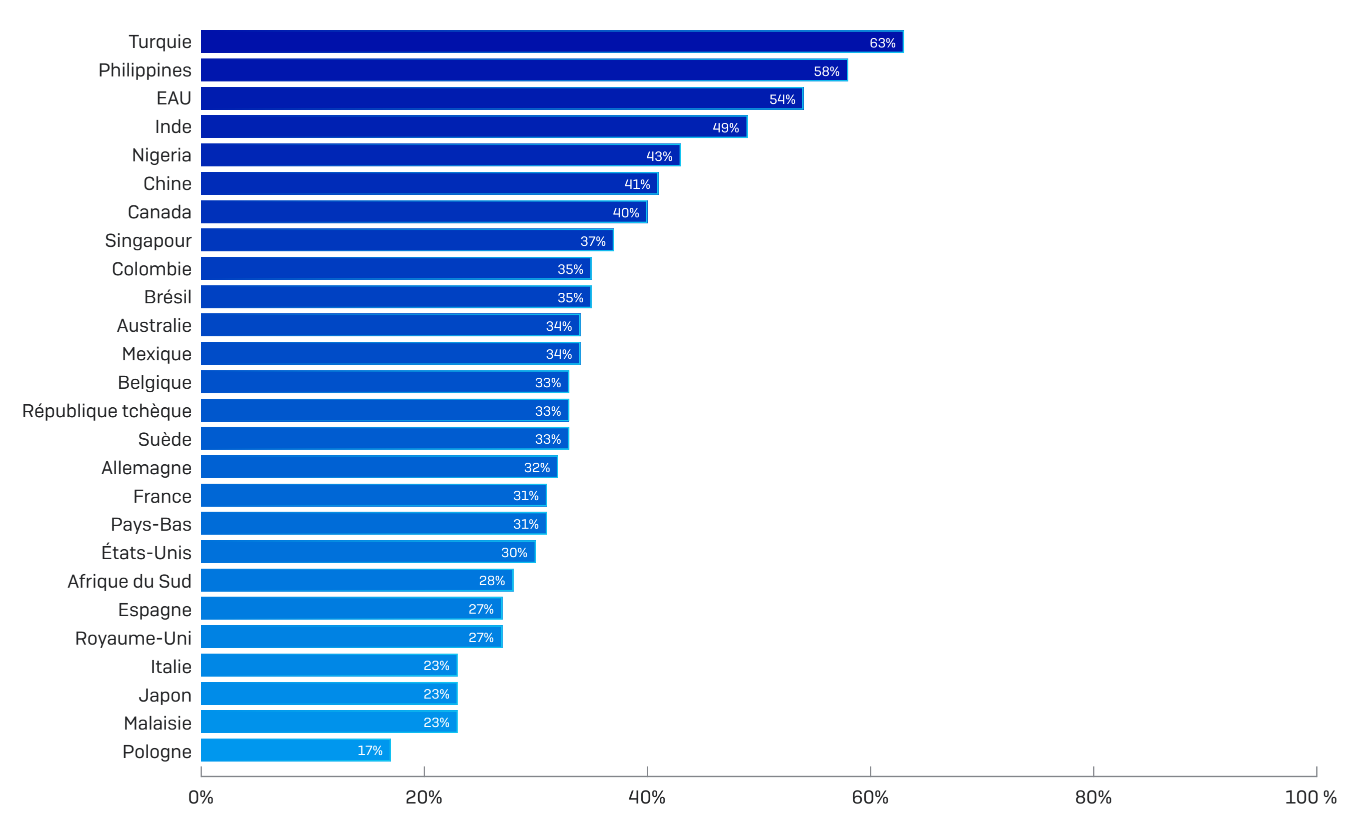
Votre entreprise a-t-elle subi un incident de sécurité dans le Cloud public au cours des 12 derniers mois ? Combinaison de réponses « Oui » (« Oui, malware », « Oui, données exposées », « Oui, ransomware », « Oui, compte compromis » et « Oui, cryptojacking ».) Base de 3 521 répondants.

- **L'Inde** (227 répondants) est le pays le plus touché avec 93 % des entreprises déclarant avoir subi une cyberattaque l'année dernière, malgré 92 % d'entre elles assurant avoir une visibilité complète sur leurs ressources Cloud. Ces chiffres indiquent un manque dans l'hygiène informatique, créant ainsi des faiblesses dans les configurations de sécurité Cloud, fragilisant les entreprises face aux attaques.
- Cette tendance est observée dans toute la région **Asie-Pacifique (APAC)**, qui présente les taux régionaux les plus élevés de données exposées (35 %), d'attaques de ransomware (37 %) et de comptes compromis (33 %) parmi les répondants.
- **L'Europe** (1259 répondants) doit certainement son faible taux d'attaques au RGPD, car les répondants européens affichent le plus faible pourcentage d'incidents de sécurité au cours de l'année passée parmi toutes les entreprises interrogées. Cela inclut l'Italie (45 %), la Pologne (47 %), l'Espagne (57 %), le Royaume-Uni (61 %) et l'Allemagne (61 %).

L'importance de la protection des données et la médiatisation de certaines attaques de ransomware ont sans doute amené ces cibles lucratives à mieux se protéger que dans d'autres régions. Ainsi, l'Europe affiche les taux les plus faibles d'infections par malwares (29 %), de données exposées (24 %) et d'attaques de ransomware (22 %) parmi les répondants. Cela explique également les taux comparatifs plus élevés de comptes compromis (21 %) et de cryptojacking (15 %), les attaquants s'efforçant d'exploiter les ressources mal configurées et les rôles IAM surprivilégiés pour compromettre les environnements Cloud.

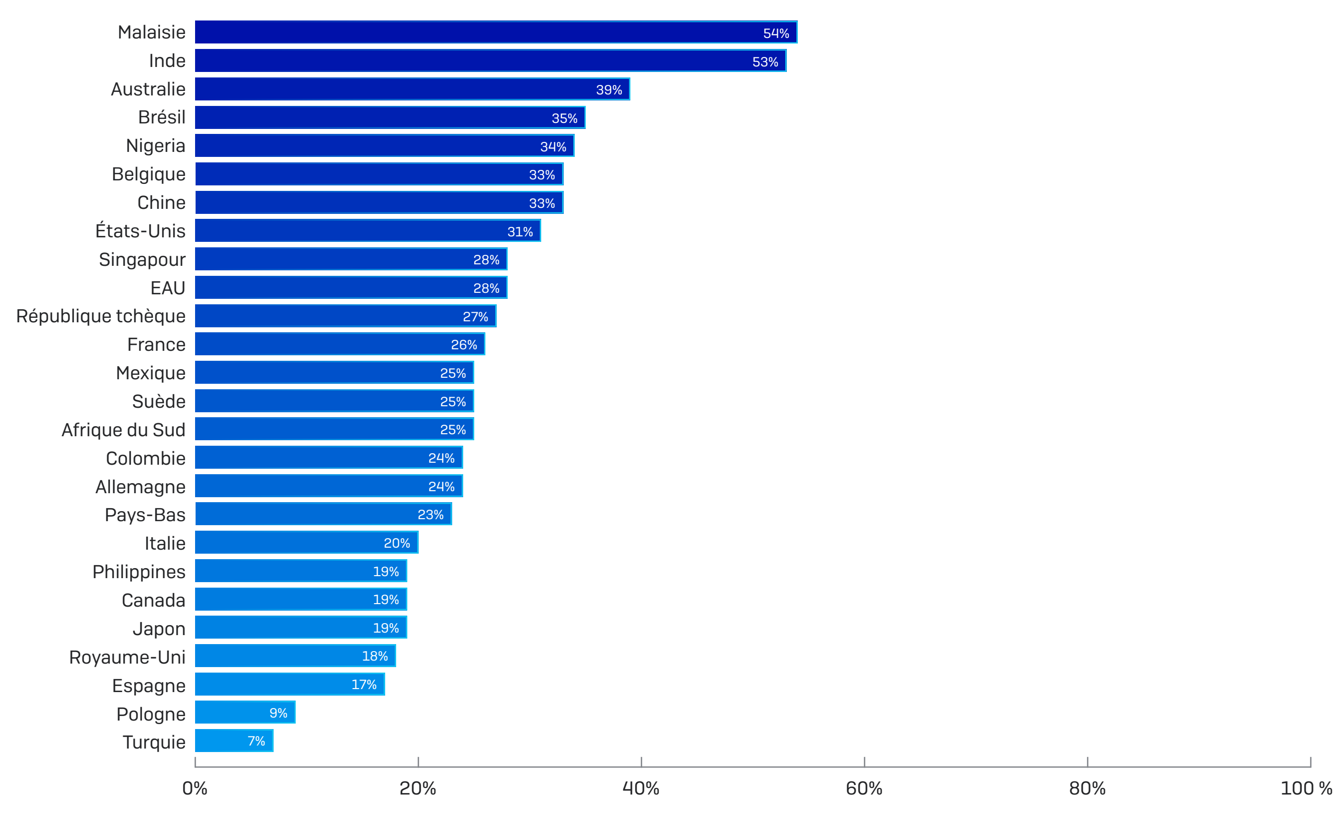
- **Le Moyen-Orient et l'Afrique** (360 répondants) ont l'un des taux d'attaque les plus faibles en dehors de l'Europe. Cela peut s'expliquer par un choix géographique des criminels qui privilégient des opportunités plus lucratives dans d'autres régions. Mais la valeur des entreprises dépend de la personne qui s'y intéresse. Ici, le cryptojacking est le plus fort parmi toutes les régions (22 %), les criminels faisant tourner des centaines de serveurs virtuels pour effectuer des opérations de cryptominage illégales et s'échapper avant d'être découverts.
- **Les États-Unis** (413 répondants) ont étonnamment déclaré peu d'incidents, bien qu'ils constituent le plus grand groupe de répondants. Ils figurent parmi les 35 % de pays ayant subi le moins d'incidents de sécurité au cours de l'année passée. En tant que pays occidental, il devrait être considéré comme une cible lucrative, pourtant seulement 30 % des répondants déclarent avoir été touchés par un malware, 31 % par un ransomware, 28 % par une violation de données et 21 % par le vol d'identifiants de compte. Les facteurs inhérents à cette situation montrent une appropriation claire de la sécurité par les entreprises, avec 90 % d'entre elles comprenant leur responsabilité en matière de sécurité Cloud. Avec 85 % des entreprises conscientes de tous leurs assets dans le Cloud, les États-Unis ont 17 points de pourcentage de plus que la moyenne mondiale.

Entreprises touchées par un malware dans le Cloud public au cours de l'année passée



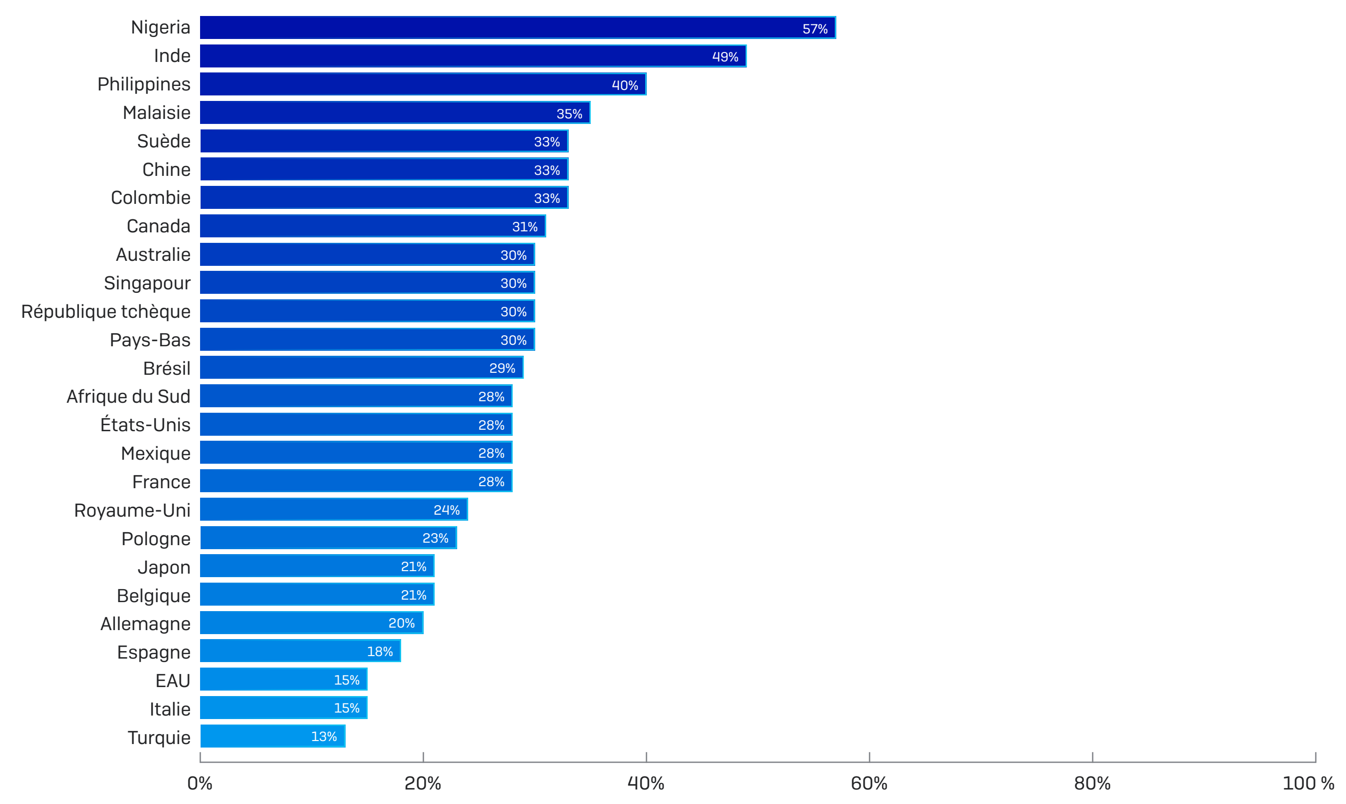
Votre entreprise a-t-elle subi un incident de sécurité dans le Cloud public au cours des 12 derniers mois ? « Oui, malware ». Base de 3 521 répondants.

Entreprises touchées par un ransomware dans le Cloud public au cours de l'année passée



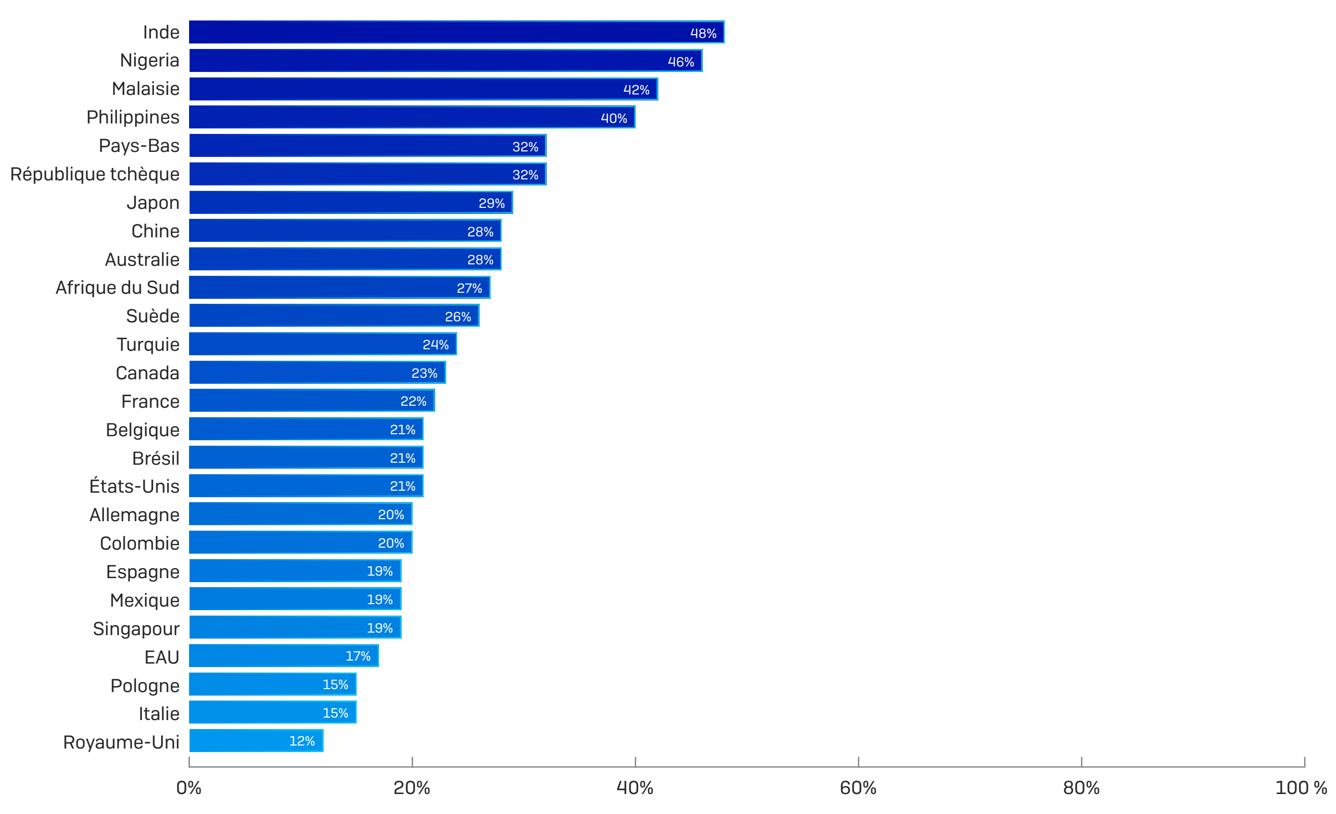
Votre entreprise a-t-elle subi un incident de sécurité dans le Cloud public au cours des 12 derniers mois ? « Oui, ransomware ». Base de 3 521 répondants.

Entreprises dont les données dans le Cloud public ont été exposées au cours de l'année passée



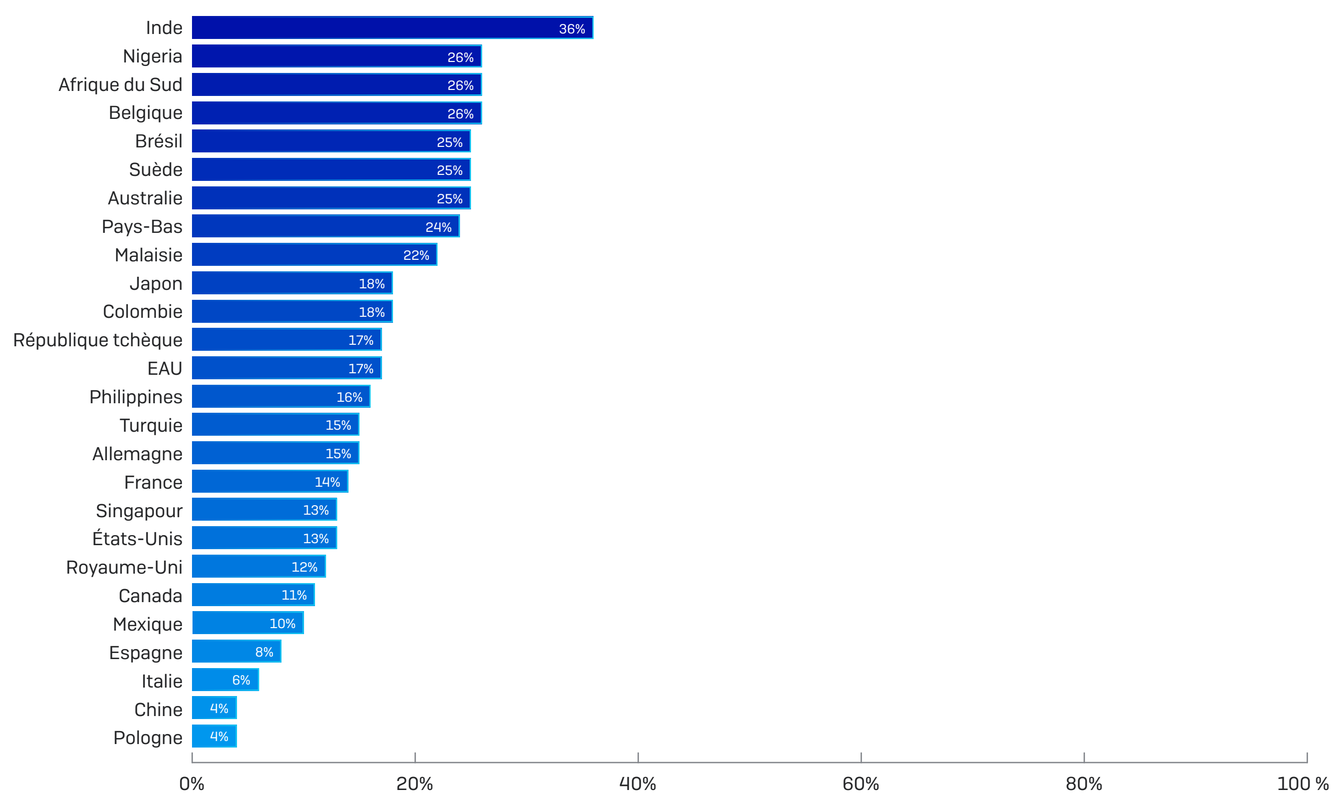
Votre entreprise a-t-elle subi un incident de sécurité dans le Cloud public au cours des 12 derniers mois ? « Oui, données exposées ». Base de 3 521 répondants.

Entreprises dont les identifiants de compte Cloud ont été volés au cours de l'année passée



Votre entreprise a-t-elle subi un incident de sécurité dans le Cloud public au cours des 12 derniers mois ? « Oui, identifiants volés ». Base de 3 521 répondants.

Entreprises ayant connu une attaque de cryptojacking dans le Cloud public au cours de l'année passée



Votre entreprise a-t-elle subi un incident de sécurité dans le Cloud public au cours des 12 derniers mois ? « Oui, cryptojacking ». Base de 3 521 répondants.

Partie 2 : Comment les criminels parviennent à entrer

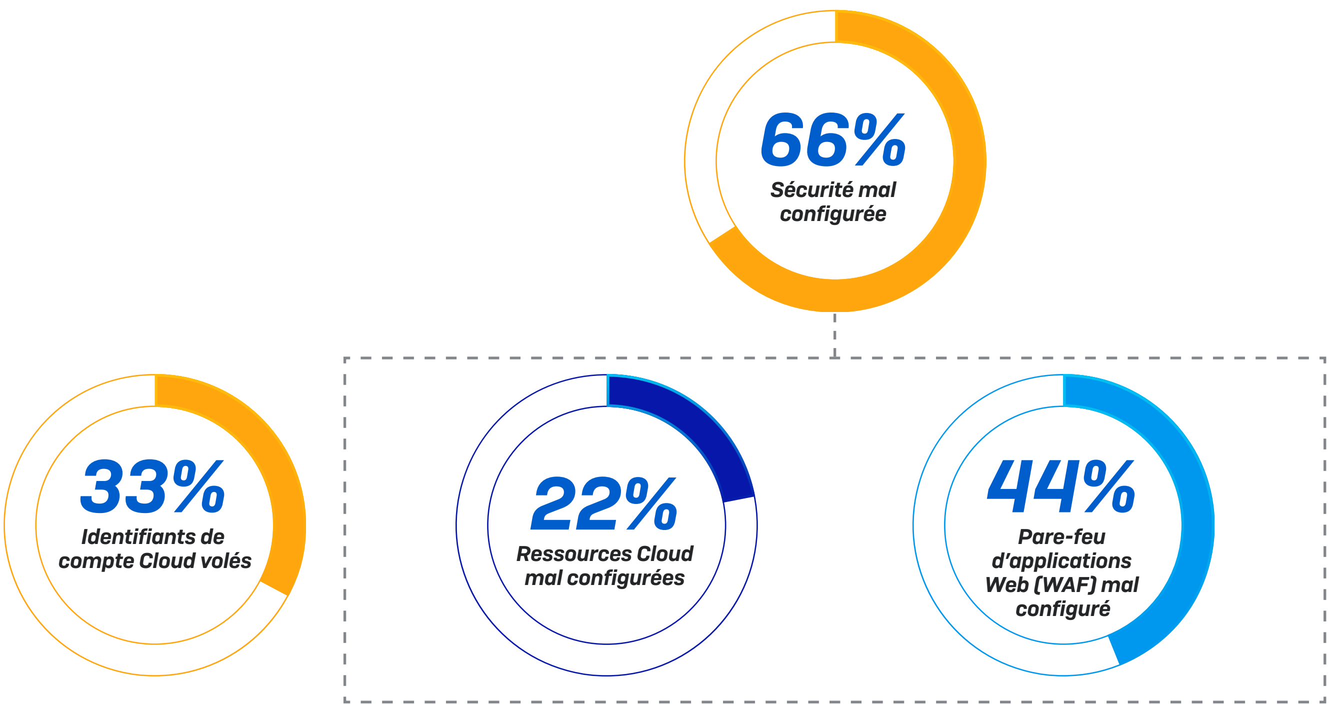
2/3 des entreprises avaient des portes dérobées ouvertes

Quand on parle du Cloud, on peut comparer le réseau à un bâtiment avec de nombreuses portes, fenêtres et autres ouvertures vers l'extérieur. Autant de points d'accès pouvant potentiellement être utilisés par quelqu'un, ou quelque chose, pour entrer dans le bâtiment et en sortir.

Par exemple, une table d'itinéraire mal configurée sur un pare-feu de l'entreprise laisse une fenêtre ouverte. Ainsi, des machines virtuelles exécutant des charges de travail dans le Cloud privé ou hébergeant des données sensibles deviennent accessibles depuis Internet.

L'exposition accidentelle continue d'être un problème majeur pour les entreprises, ce qui transparait dans les réponses de notre enquête. Les failles de sécurité causées par des erreurs de configurations ont été exploitées dans 66 % des attaques, tandis que 33 % des attaques ont utilisé des identifiants volés pour accéder aux comptes des fournisseurs de Cloud.

À mesure que les entreprises utilisent de nouveaux services Cloud afin de fournir un stockage partagé, des conteneurs, des services de base de données ou des fonctions sans serveur, le risque d'erreurs de configuration ne fait qu'augmenter, ce qui, à son tour, augmente la surface d'attaque des entreprises.



Comment l'attaquant est-il entré dans votre environnement ? Base de 3 521 répondants.

Les méthodes d'entrée varient selon les pays

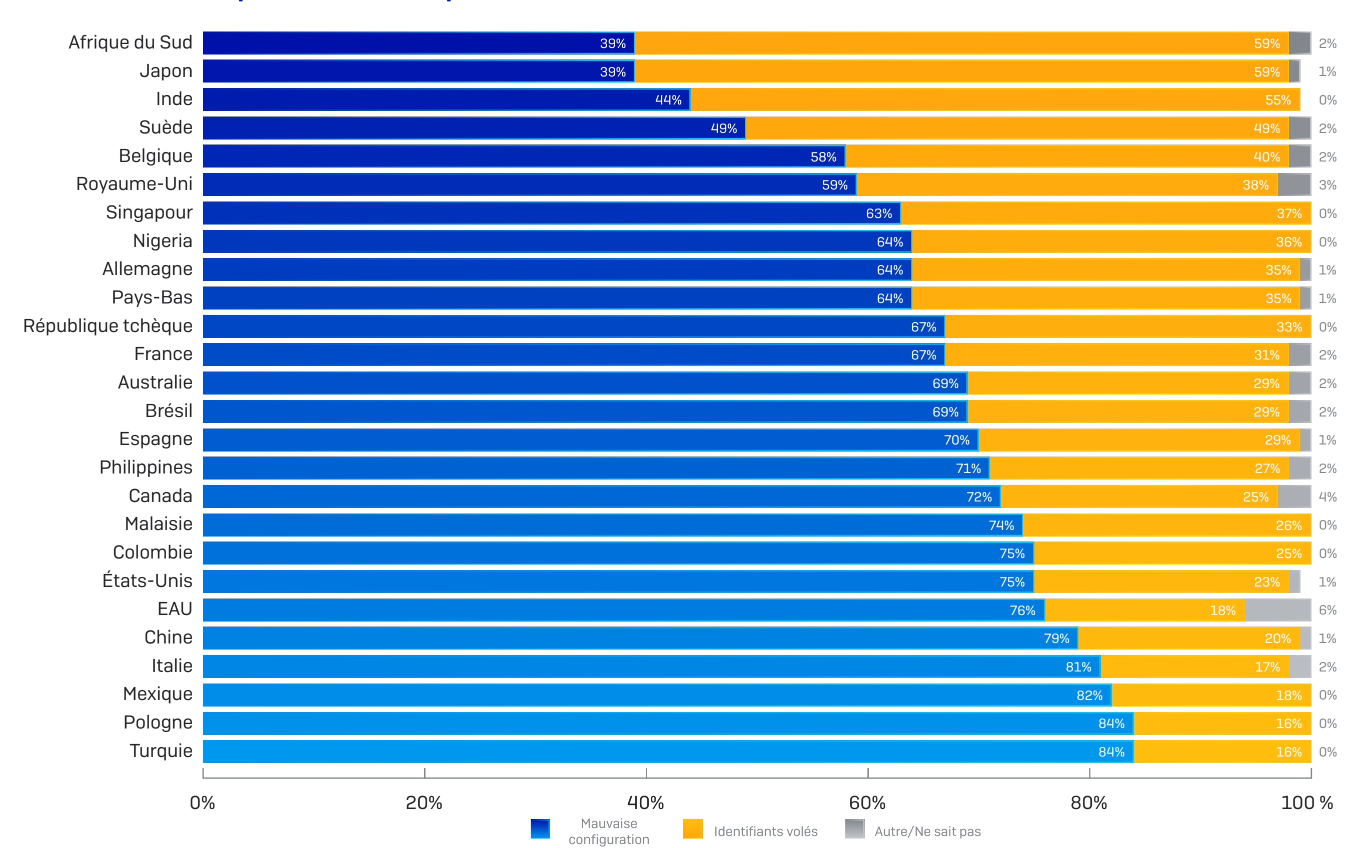
Chaque entreprise a de la valeur aux yeux des cybercriminels. Ces derniers peuvent être intéressés par les données qu'ils pourront revendre ou prendre en otage contre rançon. Ils peuvent aussi être intéressés par le portefeuille numérique de l'entreprise qui sert à payer les machines virtuelles pour le cryptominage. Et si, dans le monde réel, les cybercriminels ciblent préférentiellement leurs victimes en fonction du PIB du pays ou du secteur industriel, cela n'est pas forcément le cas dans le Cloud.

La posture de sécurité d'une entreprise est souvent déterminante dans le choix de la méthode d'entrée et des points faibles (mauvaise configuration 66 % ou identifiants 33 %). Mais il est important de comprendre que même si des erreurs de configuration offrent aux cybercriminels un accès aux comptes Cloud, celui-ci peut expirer rapidement : jusqu'à 6 heures environ lorsque des identifiants temporaires sont obtenus grâce à une erreur de configuration des ressources, par exemple.

Notre enquête souligne également le rôle de la visibilité des ressources Cloud dans la manière dont sont ciblées les entreprises :

- L'**Afrique du Sud** et le **Japon** ont révélé le nombre le plus élevé de vols d'identifiants de comptes de fournisseurs de services Cloud dans notre enquête. Ces entreprises ont également l'un des niveaux de visibilité des ressources dans les environnements Cloud les plus hauts, ce qui suggère une posture de sécurité globalement plus forte avec moins de risques d'erreurs de configuration.
- La **Turquie** et la **Pologne** montrent l'inverse : avec les niveaux de visibilité les plus faibles, ces entreprises sont les plus susceptibles d'être attaquées via des ressources Cloud mal configurées.

Comment les entreprises ont été compromises



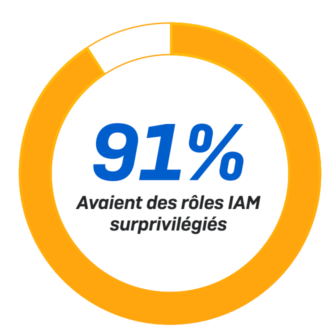
Comment l'attaquant est-il entré dans votre environnement ? Base de 2 456 répondants. En raison des arrondis, il arrive que la somme des totaux ne soit pas égale à 100 %.

La protection de l'identité est un défi de taille

Un examen des comptes Cloud par Sophos Cloud Optix, le service de gestion de la posture de sécurité du Cloud, a révélé des tendances inquiétantes dans la posture de sécurité des entreprises en ce qui concerne l'accès aux comptes Cloud.

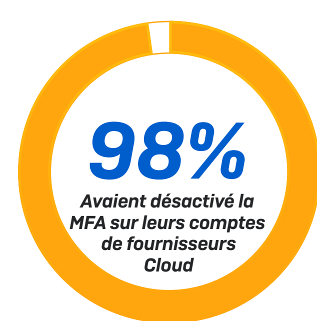
33 % des entreprises ont déclaré que les cybercriminels avaient obtenu l'accès en volant des identifiants de comptes Cloud. Une fois à l'intérieur, cependant, toutes les attaques ont utilisé les rôles et les autorisations IAM pour naviguer sur les comptes Cloud compromis. La gestion de l'accès aux comptes Cloud est un énorme défi et pourtant, seul 1/4 des entreprises interrogées dans le cadre de notre enquête y voient un sujet de préoccupation majeur.

L'ampleur et la nature imbriquée de l'accès individuel et de l'accès de groupe aux services Cloud ne permettent pas toujours aux entreprises d'avoir une visibilité détaillée sur la manière dont ces services sont accédés, et ce manque de visibilité est exploité par les attaquants.



Pourquoi c'est important

Accorder aux utilisateurs, groupes et services Cloud IAM des autorisations d'accès étendu est une pratique risquée. Si ces identifiants devaient être compromis, alors les cybercriminels pourraient avoir accès à tous les services et à toutes les données accessibles grâce à ces autorisations.



Pourquoi c'est important

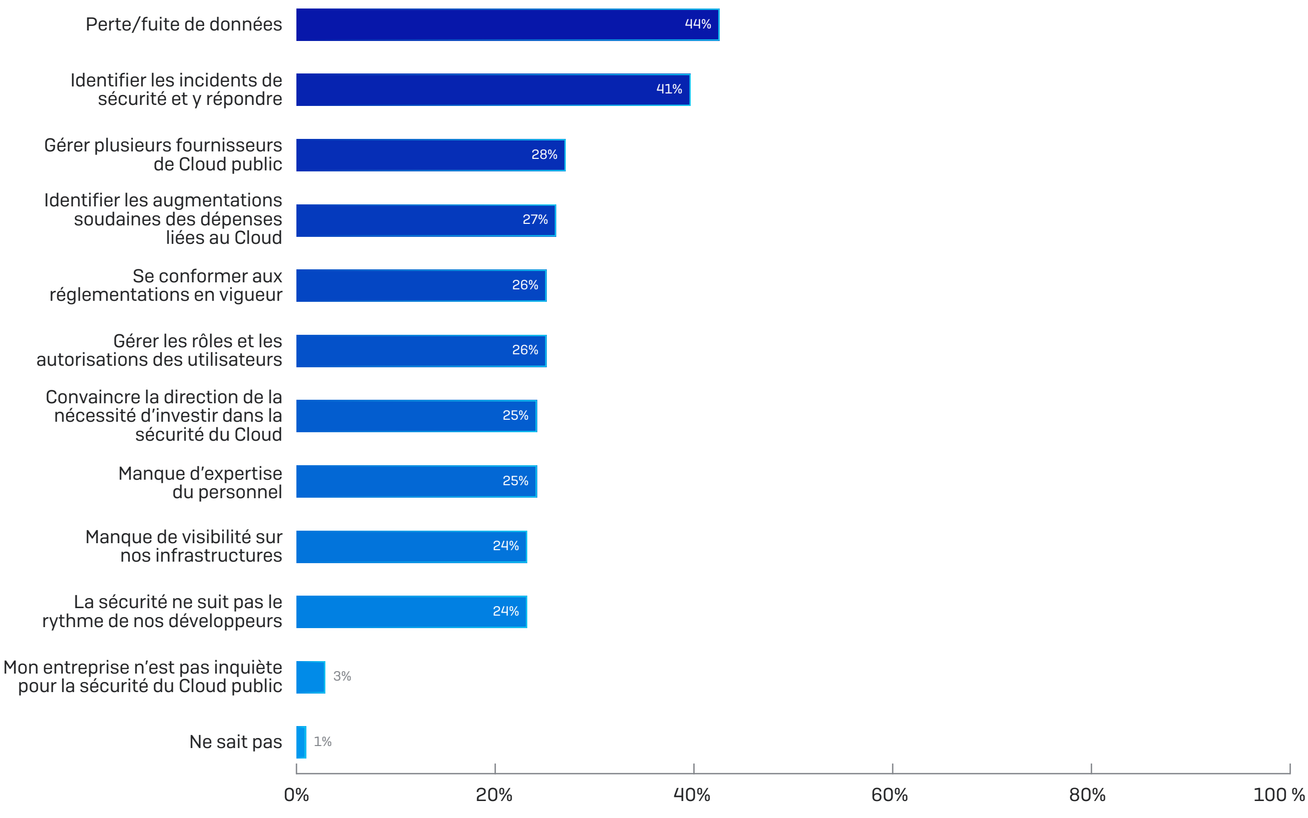
Tous les comptes utilisateur devraient avoir la MFA (authentification multifacteur) activée afin d'empêcher le vol des mots de passe. La MFA ajoute une couche de protection supplémentaire, en plus des identifiants et des mots de passe.

Partie 3 : Les entreprises ne se préoccupent pas de l'origine du problème

La perte de données est la conséquence la plus préoccupante pour les entreprises

La sécurité des données est en tête de liste des préoccupations, citée par 44 % des répondants. La nette augmentation de l'utilisation du Cloud a fracturé la distribution des données, avec 73 % des entreprises utilisant désormais au moins 2 plateformes de Cloud public. Cette approche multi-plateforme aggrave le problème de visibilité pour les équipes de sécurité, qui doivent souvent passer d'une plateforme à l'autre pour obtenir une image complète des ressources dans le Cloud.

Principales préoccupations des entreprises en matière de sécurité du Cloud



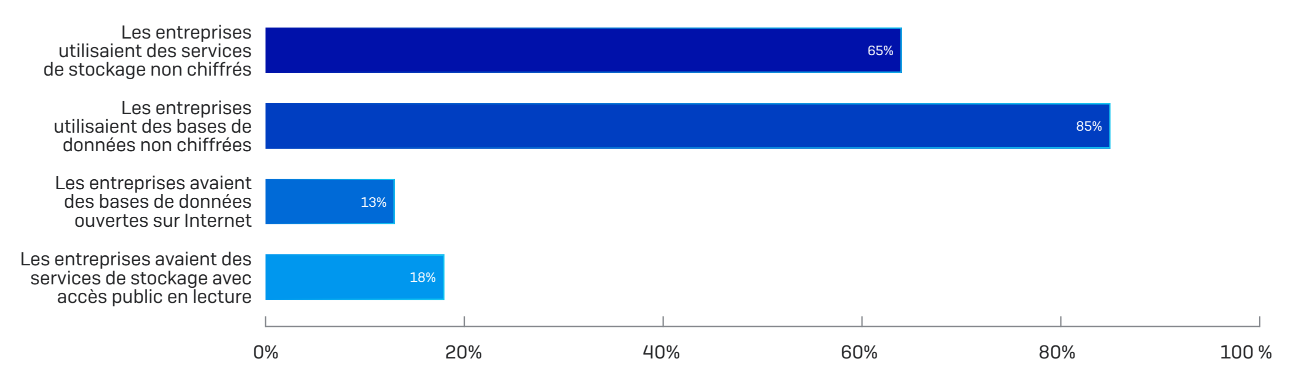
Combinaison de réponses classées en 1re, 2e et 3e position à la question : « Quelles sont les principales préoccupations de votre entreprise en matière de sécurité du Cloud public ? ». Base de 3 521 répondants.

L'une des causes principales est le manque d'expertise en matière de Cloud

Pour sécuriser correctement un environnement Cloud, une architecture adaptée et des cas d'usages clairs sont nécessaires afin d'exploiter efficacement les outils de la plateforme et de les compléter par des services tiers. Cela demande des experts compétents, soit employés directement par les entreprises, soit disponibles par l'intermédiaire de partenaires. Malheureusement, alors que 70 % des entreprises interrogées ont subi une violation de sécurité au cours de l'année passée, seul 1/4 d'entre elles considèrent le manque de compétences du personnel comme une préoccupation majeure.

L'impact des configurations sur la sécurité des données

Une analyse de comptes Cloud réalisée par l'équipe Sophos Public Cloud Security a montré que l'exposition accidentelle de données via des services de stockage mal configurés continuait de gangréner les entreprises, avec 60 % d'entre elles qui ne chiffraient pas leurs données. En agissant de la sorte, les entreprises permettent aux attaquants de rechercher et d'identifier facilement de nouvelles cibles.

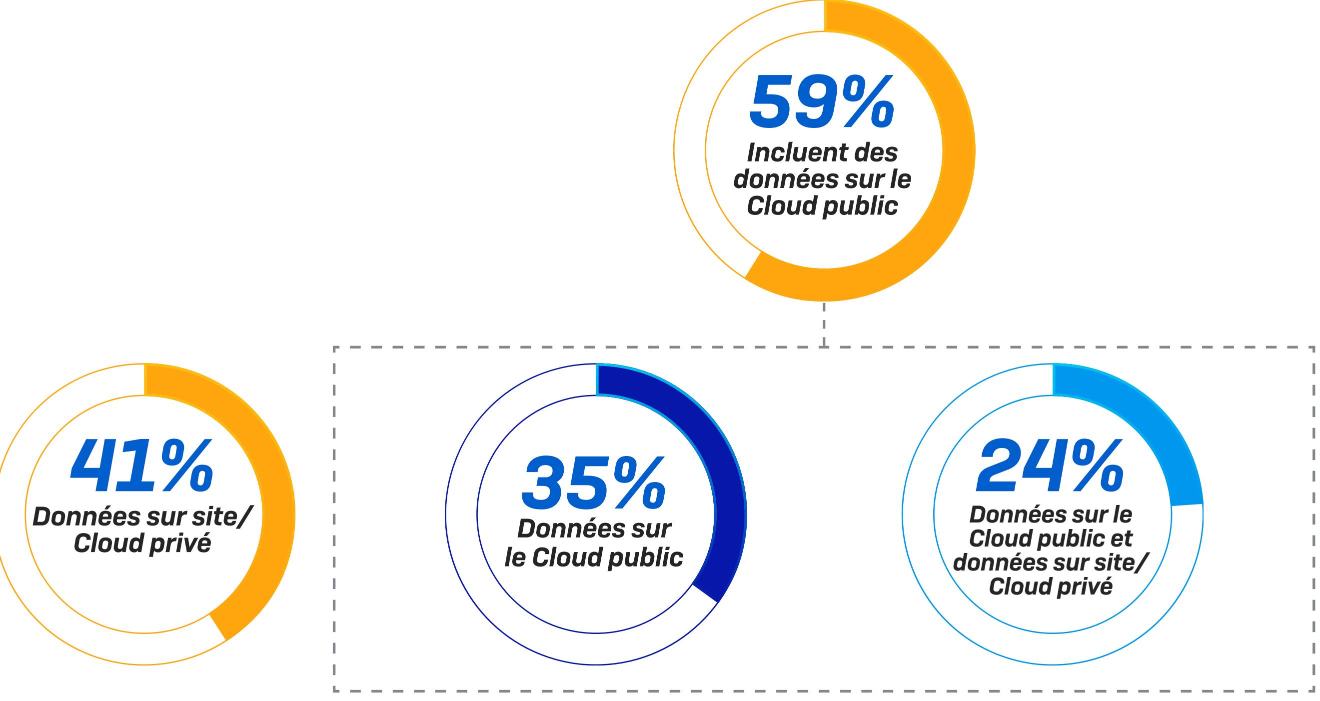


Pourquoi c'est important

Le chiffrement est essentiel pour empêcher les cybercriminels de voir et de lire les informations stockées, et il est exigé par de nombreuses normes de conformité et de bonnes pratiques de sécurité. Le « mode public », un paramètre qui peut être appliqué aux bases de données, au stockage partagé et à d'autres services de fournisseurs de Cloud, est quant à lui une autoroute vers la violation de données. Une mauvaise configuration des services Cloud en « mode public » permet aux cybercriminels d'automatiser la recherche de failles de sécurité. Des garde-fous devraient être mis en place pour empêcher de telles erreurs de configuration.

Les attaques de ransomware les plus efficaces ciblent désormais le Cloud public

Parallèlement à ce rapport sur la sécurité Cloud, Sophos a récemment publié une autre enquête menée auprès de 5 000 responsables informatiques qui s'intéressait plus particulièrement à leurs expériences avec les ransomwares. Nous avons ainsi découvert que 59 % des attaques de ransomware qui avaient réussi à chiffrer des données comprenaient des données dans le Cloud public. Bien qu'il soit fort probable que les personnes interrogées aient interprété au sens large le terme 'Cloud public', en incluant notamment les services tels que Google Drive et Dropbox et des solutions de sauvegarde telles que Veeam, il est clair que les cybercriminels ciblent les données, peu importe l'endroit où elles se trouvent.

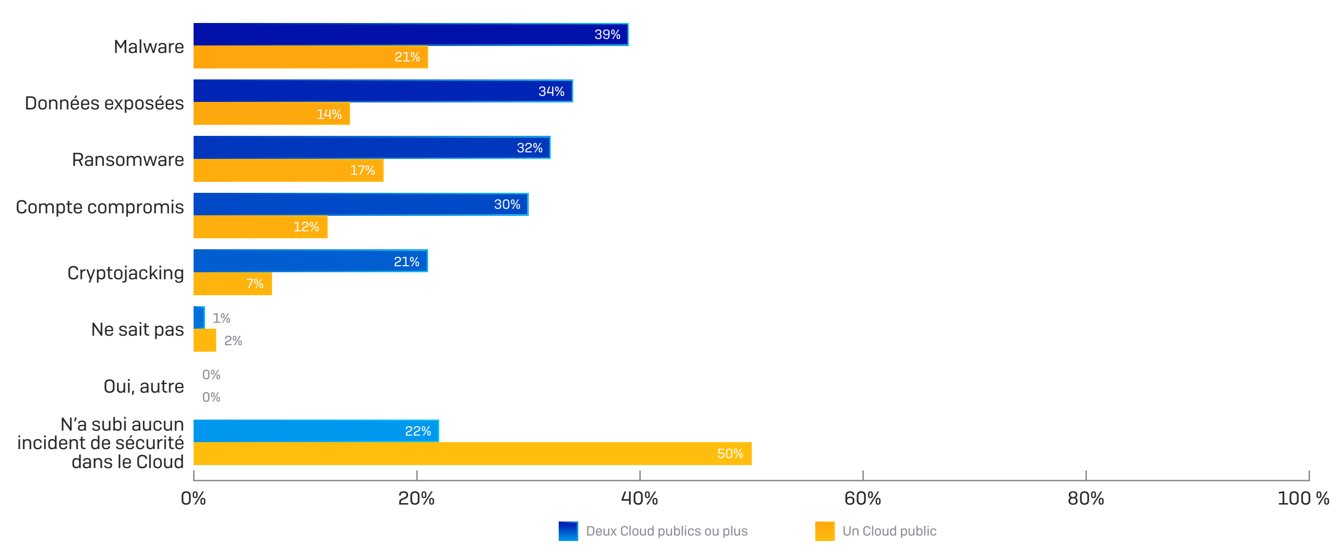


Lors de l'attaque de ransomware la plus importante, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? Les réponses viennent de répondants dont les données de l'entreprise ont été chiffrées lors de l'attaque de ransomware la plus récente. Base : 1 849 répondants.

Le multicloud crée de multiples défis

Les risques de sécurité se multiplient inévitablement à mesure que les entreprises multiplient le nombre d'environnements Cloud. 73 % des entreprises interrogées utilisent 2 plateformes de Cloud public ou plus, et ont déclaré jusqu'à 2 fois plus d'incidents de sécurité que celles n'en utilisant qu'une seule.

Entreprises avec un seul Cloud ou multicloud victimes de cyberattaques l'année passée



Les entreprises dotées de plusieurs plateformes Cloud incluent les répondants qui choisissent un ou plusieurs fournisseurs de Cloud à la question : « Dans lequel des Cloud publics suivants votre entreprise héberge-t-elle des données ou des charges de travail ? » Base de 3 521 répondants.

Le secret d'une cybersécurité efficace dans les environnements Amazon Web Services, Microsoft Azure et Google Cloud Platform consiste à améliorer la posture de sécurité globale et à traiter les aspects de la sécurité les plus importants. Il faut s'assurer que l'architecture est sécurisée et configurée correctement, obtenir une visibilité complète de l'architecture, examiner régulièrement qui a accès aux comptes et AUX services Cloud (y compris les niveaux d'autorisation) et, surtout, assurer une gestion cohérente de la sécurité dans les multiples environnements Cloud.

Recommandations

La migration des charges de travail traditionnelles vers le Cloud offre d'énormes possibilités aux entreprises de toutes tailles, néanmoins, cette enquête a confirmé qu'il est impératif de sécuriser le Cloud public. Notre étude permet de mieux comprendre comment réduire le risque d'un incident de sécurité :

1. **Partez du principe que les attaquants trouveront des ressources dans le Cloud.** Les cybercriminels automatisent désormais la recherche de services Cloud vulnérables. Qu'une entreprise utilise le Cloud depuis longtemps pour héberger des données et des charges de travail ou qu'elle ait récemment accéléré l'utilisation de services du Cloud public, obtenir une visibilité détaillée des services Cloud utilisés est la seule manière sûre de s'assurer qu'ils sont configurés de manière sécurisée et protégés contre les menaces.

2. **Investissez dans la protection des ressources Cloud avec une technologie anti-malware.** 70 % des répondants ont connu un incident de sécurité au cours de l'année passée. Parmi cette majorité, 34 % ont été touchés par un malware, 28 % par ransomware (une forme avancée de malware) et 17 % par du cryptojacking (qui peut être un malware). Ces résultats montrent que les malwares constituent la principale menace pour les entreprises et les données sensibles qu'elles détiennent.

3. **Protégez les données, en tous lieux.** La protection des données est la principale préoccupation des entreprises partout dans le monde. Près de 60 % des attaques de ransomware ayant réussi à chiffrer des données incluaient des données dans le Cloud public. Les stratégies Cloud doivent inclure la protection des données dans le Cloud public, le Cloud privé et sur site.

4. **Surveillez en continu les configurations des ressources Cloud.** 2/3 des répondants ont été compromis à cause de ressources Cloud mal configurées ; la moindre faiblesse est exploitée par les attaquants pour mener leurs activités malveillantes. Le contrôle proactif des configurations par une équipe de sécurité réduit considérablement la possibilité de violations.

5. **Gérez les accès Cloud de manière proactive.** En moyenne, les rôles IAM ont été compromis dans 33 % des cyberattaques rapportées par les répondants, allant jusqu'à 59 % dans certains pays. Pour empêcher la compromission des rôles surprivilégiés, il est essentiel de gérer efficacement les autorisations individuelles et collectives des utilisateurs.

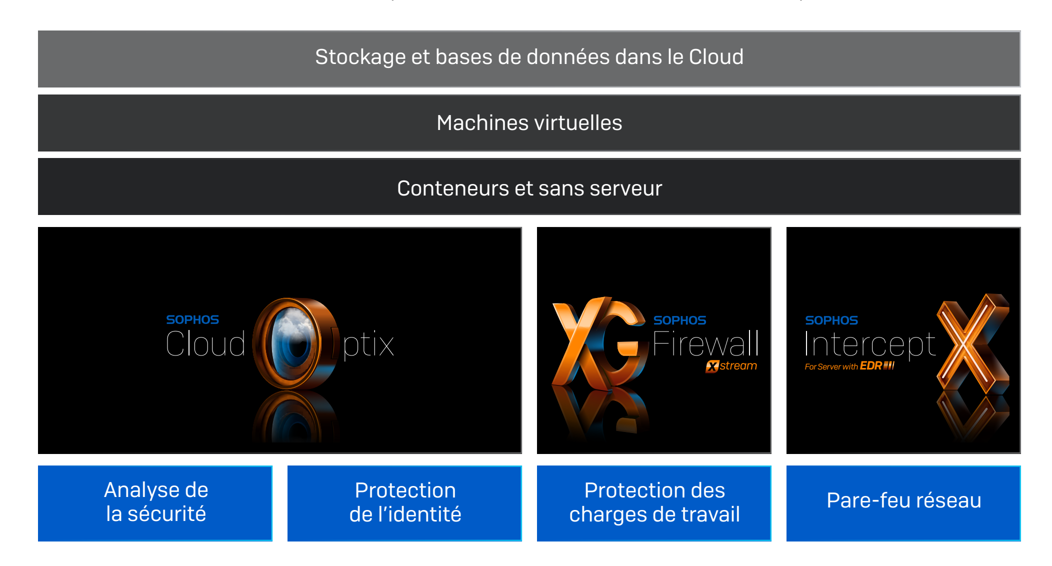
6. **Fournissez un accès distant sécurisé aux travailleurs.** Assurez-vous que vos bureaux virtuels bénéficient du même niveau de protection que les autres charges de travail critiques de serveurs. Les bureaux virtuels fonctionnent sur des machines virtuelles, qui sont exposées aux mêmes menaces. De même, comme les travailleurs à distance accèdent à des applications privées et à des données sensibles, ils devraient être équipés d'un accès VPN pour garantir des connexions sécurisées.

7. **Déployez une défense par couches.** Les cybercriminels utilisent un large éventail de techniques pour contourner les défenses. Lorsqu'une d'entre elles est bloquée, ils passent à la suivante jusqu'à ce qu'ils trouvent une faille exploitable. Assurez-vous de protéger contre tous les vecteurs d'attaque possibles.

8. **Informez-vous sur les responsabilités qui incombent à chaque partie dans la sécurisation des services des fournisseurs de Cloud public.** Les fournisseurs de Cloud public offrent une grande flexibilité. Et bien qu'ils soient responsables de la protection physique des datacenters et de la séparation virtuelle des données des clients et des environnements, les entreprises sont responsables de ce qu'elles stockent ou utilisent dans le Cloud. Près de la moitié des répondants ne comprennent pas pleinement leurs responsabilités. Pour en savoir plus, consultez les sites Web d'Amazon Web Services et de Microsoft Azure.

Sécuriser le Cloud avec Sophos

Se protéger contre la dernière génération de cyberattaques dans le Cloud public requiert un niveau supérieur de visibilité et l'automatisation de la sécurité. Sophos vous dote des technologies de protection avancées dont vous avez besoin pour neutraliser toute la chaîne d'attaque.



- **Sophos Cloud Optix** étend la détection et la réponse au niveau du Cloud public. Surveillez en continu les configurations des infrastructures Cloud pour détecter les déploiements non sécurisés, les événements d'accès suspects, les rôles IAM surprivilégiés, le trafic réseau inhabituel et les pics soudains de dépenses dans le Cloud, avec des mesures correctives guidées pour réduire les temps de réponse aux incidents. Des garde-fous verrouillent les configurations pour empêcher les changements accidentels ou malveillants qui pourraient avoir un impact sur la posture de sécurité.
- **Sophos Intercept X for Server with EDR** protège les environnements de serveur Cloud, locaux ou hybrides. Il protège les machines et bureaux virtuels Windows et Linux contre les menaces les plus récentes, notamment les ransomwares, les attaques sans fichiers et les malwares spécifiques aux serveurs. Automatisez la détection et la réponse avec une visibilité inégalée pour traquer les menaces évasives, voir et contrôler exactement quelles applications sont en cours d'exécution et répondre automatiquement aux incidents.
- **Sophos XG Firewall** protège la périphérie du réseau avec la solution de pare-feu tout-en-un ultime. Obtenez l'inspection approfondie des paquets avec VPN pour les travailleurs distants, IPS, ATP, filtrage des URL, antivirus bidirectionnel pour le WAF avec déchargement de l'authentification, routage basé sur des chemins et blocage au niveau national. La communication synchronisée avec les charges de travail dans le Cloud automatise l'isolement et le nettoyage des malwares.

Démarrez instantanément une démo à la page

www.sophos.fr/demo

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

20-06-18 WPFR (DD)

